Awareness Through Agility:
Teenagers as a Model for Terrorist Development of Situational Awareness

By Matthew J. Sheffer

Editorial Abstract:* *Mr. Sheffer observes how Allied commanders' decision making is slowed by application of strategic situational awareness concepts in tactical environments. He argues that modern teenagers present an agile, useful model of how insurgents communicate on the battlefield, and recommends military commanders adopt a similar situational awareness approach.

What do terrorists, teenagers, and the individual soldier have in common? The need for agile communications in their tactical operations.

The agility exercised by teenagers in gathering situational awareness is a model for how insurgent terrorists communicate on the battlefield. Tactical decision making by coalition commanders is slowed because they apply strategic situational awareness concepts within tactical environments. Currently, the military develops tactical situational awareness, then transfers this to the strategic common operational picture. Alternatively, the teenage communications model provides an evolutionary concept of operations, where allied forces can develop a highly flexible tactical situational awareness in urban environments by leveraging commercial technologies and infrastructure. The forced technical interoperability between tactical and strategic operations centers hinders agility at the tactical level. We must change the strategic/tactical model in our defense against terrorism, to keep pace with the enemy's rapid planning-and-attack cycle. By leveraging the teenage model—to improve the flexibility and speed at which we provide information to the urban warfare environment—we must change the "Cold War" communication paradigm. This shift will allow for more rapid development of tactics, techniques, and procedures (TTPs), which are critical in the urban warfare environment. Teenagers use situational awareness to make decisions regarding their interpersonal relationships in much the same way military and civilian leader make decisions. By using commercially available, collaborated, and highly resilient communications capabilities, both teenagers and terrorist insurgents develop situational awareness in an unconstrained manner. This article presents possible solutions to merging agility with necessary strategic/tactical secure infrastructure, to gain urban warfighting superiority. Defeating terrorist insurgents requires allied commanders to develop situational awareness with the same efficiency and agility as teenagers—and the terrorists themselves.

Technology-enabled teen. (Montclair State University)

1.0 Introduction

Effective situational awareness is essential to battlefield management. Terrorists, teenagers, and the individual soldier all require effective situational awareness to conduct operations. Terrorist situational awareness evolves through the use of covert communications. Given a finite amount of existing communications methodologies, it should be possible to discover how terrorists communicate without knowing much about the content or the sender-recipient pair. Using the teenage communications paradigm as a model, it is possible to discover the communications methodologies being employed by terrorists. Understanding how terrorists exchange information will offer coalition forces the ability to respond more effectively, by developing strategic objectives that improve the likelihood that tactical situational awareness results in improved anti-terrorism defences. Effective actions demand coalition forces gain situational awareness faster than terrorist elements.

2.0 The Teenage Communications Paradigm

Teenagers are defined as youth between the ages of 13 and 19 (inclusive). However, in American culture we can place this label on people as old as 21 or 22. Teenagers form unique social groupings that are often held together by both paranoia and friendship. Paranoia causes a teenager to gather a consistent stream of situational awareness regarding members of their clique, so that they may discern these member's motives, and react accordingly. Such intelligence, often both actual and imagined, causes teenagers to constantly readjust their TTP. For teenagers, situational awareness shapes the day-to-day structure of their social group.

A teenaged intelligence network. (Defense Link)

While they may be unaware, teenagers perform every action in the intelligence cycle[1] in order to produce their required picture. The teenage communications paradigm is primarily concerned with the collection aspect of the intelligence cycle. In order to collect situational awareness, teenagers use two technological tools—computers and cell phones—as well as human intelligence gathered through daily interactions with those around them.

It is also important to realize that teenagers primarily distribute information horizontally. By horizontally disseminating situational awareness, a teenager is able to have a greater perception of their surroundings without having to request information from "higher headquarters." Unlike the military, there is very little resistance to the flow of information between independent elements, as vertical information distribution is essentially non-existent.

2.1 Computer Based Situational Awareness

Computers have become an important resource in teenaged situational awareness development. So called "Social Networking" sites such as MySpace and Facebook have permanently changed the way teenage cliques are organized and managed. Social networking over the Internet allows for effective information gathering and denial-and-deception operations. Web logs, or blogs, have also become an integral part of information dissemination and collection. Internet sites such as Blogger, LiveJournal, and Blogspot leverage advertising revenue to provide free Internet accessible space. Instant messaging—provided by companies such as America Online (AOL Instant Messenger), Microsoft (MSN Messenger), and Yahoo! (Yahoo! Messenger)—allows for real-time communications in either a one-to-one or one-to-many mode over the Internet.[2]

2.1.1 Web-Based Social Networking

Web-based social networking allows for definition of groups online, by connecting people using a defined relationship. Two of the most popular social networking sites are Myspace.com and Facebook.com. MySpace is currently the world's fifth most popular English language Internet site.[3] MySpace allows teenagers, and anyone else with Internet connectivity, to post pictures and textual information for free. By adding other MySpace users to one's list of friends, one can define relationships, collect information and disseminate it appropriately. With MySpace it is possible to conduct "covert" collection activities on any member, without needing an account or validating an existing relationship. This allows teenagers to gain situational awareness without disclosing sources and methods.

A more structured Web-based social network is Facebook. Only teenagers with validated credentials (a college e-mail address or invitation from a previously authenticated high school student) can access Facebook content. Within Facebook, preliminary associations are made based on school affiliation; allowing for only cursory information —such as name, school affiliation, and a small user-posted picture—to be collected. Facebook's tiered security limits "covert" collection, however once a relationship has been defined, users can see all posted information regarding one another. With a sense that their content is more protected, Facebook users often post more detailed information and more unedited pictures than what might be seen on MySpace.

2.1.2 Blogging

Blogging has revolutionized the way we disseminate information. Teenagers, once seemingly averse to writing, have begun to author online journals in the form of blogs. Such authoring allows teenagers to express themselves and, in some cases, gain limited notoriety. Blogs differ from Web-based social networking sites as the information is more personal, and the publication's author may be anonymous to all but a small social group.

In both Web-based social networking and blogging, situational awareness is obtained from user-posted information and visitor comments. In Web-based social networking increased intelligence can be collected by following a trail of comments between users; much like an e-mail trail results from multiple messages sent back-and-forth among a group.

2.1.3 Instant Messaging

Instant messaging allows for short, real-time messages to be sent between users over the Internet. Numerous applications exist to exploit this capability; some of which include AOL Instant Messenger (AOL IM), MSN Messenger, and Yahoo! Messenger. The intelligence benefits of instant messaging are twofold. First, instant messaging allows for rapid, informal communications in order to disseminate or collect targeted information. Secondly, instant messaging services often allow users to post information in a profile that any user can read. Profiles are frequently updated and will often include information regarding the user's location. Intelligence collection against a number of targets makes it possible to build relationship structures, and develop situational awareness based on critical information requirements.

2.2 Cell Phone Based SA

Teenagers use three applications of cell phone technology to collect intelligence: text messaging, picture messaging, and voice communications. Text messaging allows teenagers the same rapid, informal communications as instant messaging, but without the ability to post static "profiles" that are common in instant messaging. This means cell phones are used to gather targeted intelligence by asking carefully crafted questions, or collecting intelligence via information disseminated by reliable sources. Picture messaging allows users to send an image taken from a normally low resolution camera located on the phone, to anyone with a cell phone or e-mail address capable of receiving them. Traditional voice communications are a primary collaboration means between teenagers, however this method is less agile and more time consuming than the previous two.

2.2.1 Text and Picture Messaging

Teenage use of text messaging is increasing on a daily basis. Text messaging provides them an informal way to send information such that no direct interaction with the recipient is required. Coordination of event information, brief single-topic discussions, and information verification are just some of the potential uses of text messaging among teenagers. This method changes the way that information is disseminated by reducing the energy and time expended in the exchange. As the telephone revolutionized information exchanges that once took days or weeks via the postal mail, text messaging is now poised to further reduce time-to-delivery. Texting is also a discreet form of communications, allowing for conversations in constrained environments where cell phone-based voice communications are prohibited.

Teenagers use picture messaging in the same way military organizations use imagery intelligence. Through photo interpretation, teenagers can gain situational awareness as well as provide details about the subject's location and acquaintances. Alternatively, one can also glean information about the person taking the photo. In this way a picture can often simultaneously tell a teenager who is participating in an activity, where and when that activity is taking place, and what ancillary activities are occurring.

2.2.2 Voice Communications

Teenagers love to talk on the phone. This traditional method of communications is still a primary means of information gathering. In a recent Pew Internet and American Life Project survey, 63% of teenagers surveyed reported phone-based voice communication as their primary means of collaboration with friends.[4] Voice communications over cell phones allows situational awareness gains based on more perceptual signals, such as voice inflection. Voice communications also allow dialogue to direct situational awareness. With the understanding that "you don't know what you don't know," it is often impossible to ask every question which might provide situational awareness. Dialogue between teenagers allows situational awareness development without being constrained by limited prior knowledge.

2.3 Information Dissemination

In order to be collected, information must first be disseminated. Dissemination between teenagers can be either unintended or offensive in nature. Both types of propagation can be accomplished using any of the means mentioned. This is an example of unintended intelligence dissemination among teenagers:

John, Walt, Roger, and Paige are friends and members of a social group. John wants to invite his friends to attend a concert that evening. John decides to send each friend an instant message via AOL Instant Messenger (AOL IM) in lieu of a formal invitation or phone call. An AOL IM user can exist in three states: active, inactive, and away. If a user is "away" he must leave a message that will display when another user sends a message. Away messages often describe where and with whom the user currently is (although this is not a formal requirement), and the length of time the user has been away. When John sends a message to Walt, Roger, and Paige he finds all three are away. The away messages returned to John read:

Walt: "I'm at the Bright Star Bowling Alley." [34 minutes]

Roger: "Out of the house" [34 minutes]

Paige: "Spending time with Roger and Walt" [34 minutes]

Through these away messages John is able to deduce that his friends decided to go bowling without him. This intelligence increases John's situational awareness and aids in his future decision making.

The use of offensive information is normally in the form of rumors and speculation. Such information can be posted to Web-based social networking sites, blogs, or instant messaging profiles; pictures that are taken out of context can be sent via cell phone picture messaging. Denial and deception campaigns should also be considered offensive information dissemination.

3.0 The Teenage-Terrorist Model

Describing the terrorist communications paradigm would be to repeat the teenage communications paradigm described above, with only minor changes. Terrorists have a somewhat greater need to exercise operational security (OPSEC), as coalition forces actively target their communications. This OPSEC requirement forces terrorists to employ TTPs which hide both actual communications, and individual components of their collaborative environment. Through open source analysis of these discovered communications, we can infer an analogous relationship between communications paradigms exercised by both teenagers and terrorists.

While terrorists may not use Facebook or MySpace, they have demonstrated use of the Internet for mission planning and information dissemination in the past.[5] Terrorists have also demonstrated a keen understanding of cell phone technology, making mobiles useful in both mission planning and weapons triggering.[6] Terrorists use technology in ways quite similar to teenagers. While their collaborate environments may look different from those used by teenagers, terrorists' underlying capabilities are nearly identical.

3.1 Internet Based Communications

Terrorists need covert communications between geographically disparate cells to carry out situational awareness and mission planning. The anonymity of the Internet seems to offer the widest range of services while providing the greatest OPSEC opportunities. Each Internet-based communications technology used by teenagers has been employed by terrorist elements. Continued reliance on technology as a force multiplier and agility enabler will decrease the length of the terrorist planning-and-attack cycle, and increase the ability for geographically disparate participants to engage in terrorist activities.

While not as openly commercial as those services used by teenagers, terrorist Internet usage is just as sophisticated. The Internet has improved terrorist groups' ability to gather and distribute critical information for the production of situational awareness.

3.1.1 Web-Based Social Networking

Younis Tsouli, also known as "Irhabi 007," was skilled in the art of Internet use to further the goals of Islamic fundamentalist terrorism. Using a myriad of "underground" websites and password protected chat rooms, Irhabi 007 linked numerous geographically disparate terrorist entities—and their potential recruits—via the World Wide Web. Though captured in November 2005, he had already provided all of the necessary recruiting and social networking resources required for continued terrorist use of Internet.[7]

According to TrackingTheThreat.com, which provides link analysis between suspected terrorists, many extremists can be linked even though they are located in geographically separate areas.[8] From these links, we can infer that Web-based social networking plays a part in the organization of terrorist structures.

For example, Orkut, a Web-based social networking site affiliated with Google, is gaining popularity in the Middle East. Orkut's popularity is most evident when searching through its social communities based on support for specific terrorists or terrorist networks.[9] These communities are formed much like communities on Facebook or MySpace except that rather than support for a university or sports team, the relationships are built on support for terrorism. If this trend continues to grow, extremist communities could easily create substantial recruiting and sympathizer lists.

3.1.2 Blogging

While terrorists have not demonstrated pervasive use of blog technology, a similar capability exists in message forums which are a well documented form of terrorist collaboration. Message forums allow users to post messages and have other users respond. These messages boards are often displayed in a hierarchy based on "threads." A new thread is similar to a post on a blog, while the replies to a thread are almost identical to comments left on blogs.

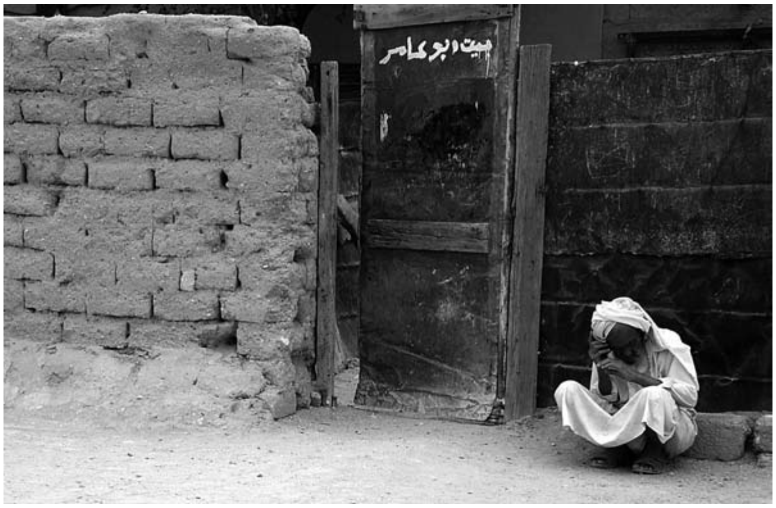
Terrorist message forums, many started by Irhabi 007, provide a continuing collaborative capability, where situational awareness can be disseminated rapidly between geographically disparate users. Extremists have been known to use message forums to collaborate on tactics and weapons; including weapons of mass destruction.[10]

3.1.3 Instant Messaging

Instant messaging allows terrorists to rapidly initiate collaborative sessions from almost any connected device. Instant messaging services offer a flexible framework for communications in a one-to-one or one-to-many collaborative environment. Due to the myriad of instant messaging service providers, it is conceivable that anonymity would be increased by "service hopping," or rapidly developing new aliases (screen names). Encryption technology also offers a measure of privacy that would be required for terrorist communications.[11] Given the technology's widespread availability, one should always expect terrorists have the potential to use instant messaging in planning and attack coordination.

3.2 Cell Phone Based Communications

Cell (or mobile) phones provide an invaluable communications tool for terrorist organizations. The prevalent use of cell phones is indicated by their discovery as both a situational awareness tool and a weapons trigger. The use of communications equipment in effects based operations has highlighted the insecurity of cell phone communications among Coalition enemies. We must also understood that terrorists have received warnings regarding cell phone usage for critical operations. However this technology is so pervasive throughout society, it would be hard to operate completely without one. Terrorists must be considered a subset of any population in which they reside. As cell phones are a common means of communication in much of the world, we must infer the



The long reach of the mobile phone. (Defense Link)

percentage of terrorists using them is roughly equivalent to the cell phone-using population of a given region.

3.2.1 Text and Picture Messaging

Text messaging is prevalent in areas where terrorists operate, however information on the use of picture messaging is generally unavailable. Terrorist use of text messaging generally seems to occur on "throw away" cell phones—cell phones either purchased using false names or used for only a short period of time.[12] Just as teenagers use text messaging to organize events, terrorists in Australia are charged with planning meetings using cell phone text messaging.[13]

The ability to rapidly disseminate information in a one-to-many manner is valuable to both terrorists and teenagers. In Iraq, the local population actively uses text messaging to report crimes to the Iraqi Police Service.[14] Given this technology is being actively used to expose terrorism, it is also likely being used to carry out terrorist acts.

3.2.2 Voice Communications

Terrorist use of wireless voice communications technology in support of situational awareness is well documented. The US National Security Agency (NSA) had Osama Bin Laden's satellite phone under surveillance, prior to the exposure of that fact. As early as 2003, security services were unraveling terrorist networks based on the phone numbers of associates stored in captured terrorist cell phones.[15] The prevalence of cell phones and their network infrastructure has only increased. While this network is under continued surveillance, it remains of importance in situational awareness gathering and dissemination.

4.0 Coalition Strategic Objectives

Correlation of the teenage communications paradigm with that of terrorists allows for development of two coalition strategic objectives (CSOs). First, mitigate the speed at which terrorists gain situational awareness by developing the same agility within coalition forces. Second, respond to the terrorist use of efficient, cost effective technology by fielding similar systems within the coalition structure. Effective CSO management will certainly result in more effective operations.

Current statistics show our tactical forces are young. Youth allows a coalition military to leverage their knowledge of situational awareness tools—such as Facebook, MySpace, blogs, and instant messaging—to mitigate agile terrorist communications methodologies. According to the Population Reference Bureau, approximately 42% of Army and Navy personnel are below the age of 25, compared with just 15% of the US civilian labor force.[16] Exploiting our military youths' pre-existing knowledge would be extremely valuable in tactical anti-terrorism environments.

4.1 Coalition Strategic Objective: Mitigate

Mitigating the speed at which terrorists gain situational awareness requires the coalition collect and disseminate situational awareness at similar speeds. Current military strategy is to coalesce situational awareness at the strategic level, requiring vertical information dissemination. The need to protect sources and methods requires some of the most important information to remain bogged down in a bureaucracy of classification.

Coalition forces conduct tactical level counter-terrorist operations on a daily basis. Due to the vertical distribution of information, tactical users often have far less situational awareness on their target than their strategic commanders. Only when we distribute information both horizontally and vertically will the tactical soldier be able to operate with critical situational awareness in-hand.

4.2 Coalition Strategic Objective: Respond

Rather than always developing technology for soldiers, the coalition should use tools that soldiers already know. Responding to the terrorist's technology requires similarly user-intuitive tools be employed at the tactical level. Coalition soldiers use, or have used, situational awareness tools throughout their young adult lives. Current military strategy is to develop technological tools because young soldiers understand technology. However, using technological tools that young soldiers already understand could be of staggering consequence. For instance, in conjunction with CSO Mitigate, what if coalition forces developed a "Terrorist Facebook" that looks and feels like today's Facebook tool used by teenagers? Armed with the same currently available tools—such as social network linking, biographical display, multiple image storage—this Terrorist Facebook would give soldiers the situational awareness needed to find terrorists in a given area of operation.

5.0 Conclusion

The teenage communications paradigm provides a model for understanding how terrorists gain situational awareness. To defeat a terrorist communications infrastructure based on tools used by teenagers, coalition military forces must use similarly agile technologies. One way to improve tactical situational awareness is to use technologies that soldiers—mostly teenagers themselves—already use and understand. Improving the agility and efficiency of coalition military situational awareness development, especially in tactical environments, will create a situation in which soldiers can respond as quickly as terrorists. It is nearly impossible to defeat an enemy who is already effectively using commercial, publicly available, Internet-based technology to gain situational awareness. However, by using similar technologies to improve horizontal information flow, it is possible for tactical forces to mitigate terrorists' operating speeds.

Notes

[1] Central Intelligence Agency, "The Intelligence Cycle," [http://www.cia.gov/cia/ciakids/who_we_are/cycle.shtml], April 2006.

[2] Duffy, Michael, "A Dad's Encounter with the Vortex of Facebook," [http://www.time.com/time/archive/preview/0,10987,1174704,00.html], March 27, 2006.

[3] Alexa Internet, "Top English Language Sites," [http://www.alexa.com/site/ds/top_sites?ts_mode=lang&lang=en], April 2006.

[4] Lenhart, Amanda et. al., "Teens and Technology," [http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf], 27 July 2005

[5] "Terrorists' Web Chatter Shows Concern About Internet Privacy," The Washington Post, 13 April 2006, A14.

[6] Appelbaum, Jacob, "IED in Iraq," [http://ioerror.livejournal.com/177534.html], April 2006.

[7] "Terrorist 007, Exposed," The Washington Post, 26 March 2006, B01.

[8] Tracking The Threat, [trackingthethreat.com], April 2006.

[9] Hunt, Kasie, "Osama Bin Laden Fan Clubs Build Online Communities," [http://www.usatoday.com/tech/news/2006-03-08-orkut-al-qaeda_x.htm], 08 March 2006.

[10] SITE Institute, "Message Posted To Jihadist Message Board provides Instruction Booklet for Home-Made Chemical Weapon," [http://siteinstitute.org/bin/articles.cgi?ID=publications12204&Category=publications&Subcategory=0], March 2004.

[11] JonyTech, "Encrypted Messenger," [http://www.johnytech.com/home.asp], April 2006.

[12] Harnden, Toby et. al., "UK Terrorists Got Cash From Saudi Arabia Before 7/7," [http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/08/07/nsaud07.xml], 08 July 2005.

[13] The Sydney Morning Herald, "The Case Against the Sydney Accused," [http://www.smh.com.au/news/national/case-against-the-sydney-accused/2005/11/14/1131951103465.html?page=fullpage#contentSwap1], 15 November 2005.

[14] Knickmeyer, Ellen, "Text Messaging Lets Iraqis Tip Authorities to Attacks From a Safe Distance," [http://www.sfgate.com/cgi-bin/article.cgi?f=/news/archive/2005/01/21/international1353EST0546.DTL], 21 January 2005.

[15] Isikoff, Michael et. al., "Like Clockwork," [http://www.msnbc.msn.com/id/5821599/site/newsweek/], 25 August 2004.

[16] Segal, David et. al., "America's Military Population," [http://www.prb.org/Template.cfm?Section=Population_Bulletin1&template=/ContentManagement/ContentDisplay.cfm&ContentID=12460], December 2004.